

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Gunnar Hamber

For: SECURE DOMAIN NETWORK

the specification of which is attached hereto.

Assistant Commissioner for Patents  
Washington, D.C. 20231

**AMENDMENT ACCOMPANYING NEW APPLICATION TRANSMITTAL**

---

**CERTIFICATION UNDER 37 C.F.R. 1.10\***  
(Express Mail label number is mandatory.)  
(Express Mail certification is optional.)

I hereby certify that this paper is being deposited with the United States Postal Service on this date January 15, 2002, in an envelope as "Express Mail Post Office to Addressee," Mailing Label Number EV005525141US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Judith Schick

(type or print name of person mailing paper)



Signature of person mailing paper

**WARNING:** Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

**\*WARNING:** Each paper or fee filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. 1.10(b).

"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

(Amendment Accompanying New Application Transmittal [4-4])

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the matter of: Gunnar Hamber

Serial No.:

Filed: herewith

For: SECURE DOMAIN NETWORK

Assistant Commissioner for Patents  
Washington, DC 20231

AMENDMENT ACCOMPANYING NEW APPLICATION

Sir:

Please amend the accompanying application as follows:

In the claims:

On page 15, line 1, change "Claims" to -- What is claimed  
is: --.

Rewrite the following claims:

3. (Amended) A system according to claim 1, wherein the access key pair is arranged to directly access the authenticated user to the parts of the secure domain (70, 80) corresponding to a user-level of privilege, thus enabling an on-line real-time provision of applications and services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).

Express Mail No. EV005525141US

4. (Amended) A system according to claim 1, wherein the access key pair is arranged to enable the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures according to a preset level of priority, access or security requirements in the security domain in real-time.

5. (Amended) A system according to claim 1, wherein the access server (60) is arranged to provide and store at least one new access key pair for each user-attempt to access the secure domain (70, 80), allowing a user (10) only one access attempt to a domain (70, 80) with the same access key pair.

6. (Amended) A system according to claim 1, wherein the access server (60) is arranged to provide at least one previously stored access key pair for additional authority-requests to the domain (70, 80) following an initial domain authorization.

7. (Amended) A system according to claim 1, wherein the access key pair is comprised in a virtual smart card.

8. (Amended) A system according to claim 1, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for

authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

10. (Amended) A system according to claim 1, having an interface to an authority (30) for validating user-credentials.

11. (Amended) A system according to claim 2, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

12. (Amended) A system according to claim 2, wherein the user-level of privilege is determined by the user certificate data and user identification data.

13. (Amended) A system according to claim 2, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.

16. (Amended) A method according to claim 14, wherein the access key pair directly accesses the authenticated user to the parts of the secure domain (70, 80) corresponding to the user-level of privilege, thus enabling an on-line real-time provision of applications and services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).

17. (Amended) A method according to claim 14, wherein the access key pair enables the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures according to a preset level of priority, access or security requirements in the secure domain in real-time.

18. (Amended) A method according to claim 14, wherein an access server (60) provides and stores at least one new access key pair for each user-attempt to access the secure domain (70, 80), allowing a user (10) only one access attempt to a domain with the same access key pair.

19. (Amended) A method according to claim 14, wherein an access server (60) provides at least one previously stored access key pair for additional authority-requests to the domain (70, 80) following an initial domain authorization.

20. (Amended) A method according to claim 14, wherein the access key pair is comprised in a virtual smart card.

21. (Amended) A method according to claim 14, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for

authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

23. (Amended) A method according to claim 14, wherein user-credentials are validated via an interface (30) to an authority.

24. (Amended) A method according to claim 14, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

25. (Amended) A method according to claim 14, wherein the user-level of privilege is determined by the user-certificate data and user-identification data.

26. (Amended) A method according to claim 14, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.

#### REMARKS


This preliminary amendment makes changes to delete multiple dependencies in the claims of the above-referenced patent application.

Respectfully submitted,

Dated:

1/15/2002

By

  
K. Bradford Adolphson  
Attorney for Applicant  
Registration No. 30,927

WARE, FRESSOLA, VAN DER SLUYS  
& ADOLPHSON LLP  
Bradford Green, Building Five  
755 Main Street, P.O. Box 224  
Monroe, Connecticut 06468  
Telephone: (203) 261-1234  
Facsimile: (203) 261-5676

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

On page 15, line 1 "Claims" has been changed to -- What is claimed is: --.

Claims 3-8, 10-13, 16-21 and 23-36 have been rewritten as follows:

3. A system according to [one of claims 1-2] claim 1, wherein the access key pair is arranged to directly access the authenticated user to the parts of the secure domain (70, 80) corresponding to a user-level of privilege, thus enabling an on-line real-time provision of applications and services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).

4. A system according to [one of claims 1-2] claim 1, wherein the access key pair is arranged to enable the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures according to a preset level of priority, access or security requirements in the security domain in real-time.



5. A system according to [one of claims 1-4] claim 1, wherein the access server (60) is arranged to provide and store at least one new access key pair for each user-attempt to access the secure domain (70, 80), allowing a user (10) only one access attempt to a domain (70, 80) with the same access key pair.

6. A system according to [one of claims 1-4] claim 1, wherein the access server (60) is arranged to provide at least one previously stored access key pair for additional authority requests to the domain (70, 80) following an initial domain authorization.

7. A system according to [one of claims 1-6] claim 1, wherein the access key pair is comprised in a virtual smart card.

8. A system according to [one of claims 1-6] claim 1, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

10. A system according to [one of claims 1-9] claim 1, having an interface to an authority (30) for validating user-credentials.

11. A system according to [one of claims 2-10] claim 2, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

12. A system according to [one of claims 2-11] claim 2, wherein the user-level of privilege is determined by the user certificate data and user identification data.

13. A system according to [one of claims 2-12] claim 2, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.

16. A method according to [one of claims 14-15] claim 14, wherein the access key pair directly accesses the authenticated user to the parts of the secure domain (70, 80) corresponding to the user-level of privilege, thus enabling an on-line real-time provision of applications and services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).

17. A method according to [one of claims 14-15] claim 14, wherein the access key pair enables the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures

according to a preset level of priority, access or security requirements in the secure domain in real-time.

18. A method according to [one of claims 14-17] claim 14, wherein an access server (60) provides and stores at least one new access key pair for each user-attempt to access the secure domain (70, 80), allowing a user (10) only one access attempt to a domain with the same access key pair.

19. A method according to [one of claims 14-17] claim 14, wherein an access server (60) provides at least one previously stored access key pair for additional authority-requests to the domain (70, 80) following an initial domain authorization.

20. A method according to [one of claims 14-19] claim 14, wherein the access key pair is comprised in a virtual smart card.

21. A method according to [one of claims 14-19] claim 14, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

23. A method according to [one of claims 14-22] claim 14, wherein user-credentials are validated via an interface (30) to an authority.

24. A method according to [one of claims 14-23] claim 14, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

25. A method according to [one of claims 14-23] claim 14, wherein the user-level of privilege is determined by the user-certificate data and user-identification data.

26. A method according to [one of claims 14-23] claim 14, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.